My Abdelkader Youssefi* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.3, Issue No.6, October - November 2015, 2493 – 2497.

Securing Cloud Computing Services Using Strong User Authentication With Local Certification Authority

MY ABDELKADER YOUSSEFI
Laboratoire d'Electronique et de Communications - LEC
Ecole Mohammadia d'Ingénieurs - EMI
Université Mohamed V de Rabat –UM5R
BP 765, avenue Ibn Sina Agdal 10000
Rabat, Morocco

Abstract—**Cloud computing technology provides services, computing, and storage for users over internet. This new technology allows companies to reduce hardware and software investments, users can collaborate easily with others everywhere in the world. However, security is a serious concern for cloud users. Strong user authentication is required for cloud computing in order to restrict illegal access to cloud services. In this regard, this paper proposes a strong user authentication based on digital certificates for cloud computing, users are authenticated using private public key infrastructure (PKI). The proposed method provides identity control, mutual authentication, session key establishment between the users and the cloud server. Moreover, our approach doesn't require any investment in subscription or purchasing commercial certificates for an enterprise with worldwide branches.**

Keywords- **Cloud computing, security, authentication, digital signature, public key infrastructure, certification authority**

I. INTRODUCTION

In the last few years, many enterprises have always trusted only inside users to the home network, and managed to share physical resources inside the organization. Today, companies also desire strongly to share resources they have stored in their home network devices or outside devices with users everywhere over internet. Cloud computing technology provides the facility to access shared resources over public network to perform operations that meet changing business needs. The location of physical resources is typically not known to the end users [1, 2]. It also provides facilities for users to manage their applications on the cloud, with remote access connections. This remote access raises major concern related to authentication of users and/or service provider. User authentication is the first step for access control, in the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the internet. This concern has attracted the attention of researcher, and some techniques have been proposed. The first technique used for authentication of remote users was conventional knowledge based on simple login and password, but this way is today insufficient to ensure strong security for important cloud services. This technique requires less effort for attackers to steal login and password [3]. Subsequently, strong user authentication methods have been developed to improve the strength of an authentication system. Strong user authentication approach is today the best solution to secure access to services for cloud based platforms. Strong user authentication refers to combination of two or more classes of human authentication factors:

- Something known to only the user (knowledge based): password, shared secrets, PIN…;
- Something held by only the user (possession based): security token, smart card, mobile device...;
- Something inherent to only the user (biological or behavior biometric): facial recognition, fingerprint, voice recognition…

The combination of the two known and held factors makes up the strong user authentication method, and significantly improves the authentication strength, as it secure against the threat of stolen digital identities [4]. However, not all of the available strong authentication techniques that are available today lend themselves well to the cloud computing services. Conventional strong authentication methods that involve the deployment of hardware tokens, such as smart cards are useful for closed communities such as employees and partners of one organization. Moreover, these strong user authentication methods are difficult to manage and too costly for cloud computing environment [5].

In this paper, we propose a new solution for strong user authentication, our approach is relatively cost effective to implement for cloud based services. Our technique is based on local certification authority and digital signatures. Digital signatures can be used to authenticate the source of messages. A

digital signature is a mathematical scheme to verify the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message. When a digital signature secret key is affected to a specific user, a valid signature shows that the message was sent by that user [6, 7]. Proposed method improves the authentication strength without any hardware tokens that can be costly and difficult to manage.

This paper is organized as follows. Section 2 presents user authentication in cloud computing services. In Section 3, the knowledge based authentication (KBA) is introduced. One time passwords (OTP) are described in Section 4. In Section 5, the authors investigate the conventional strong user authentication in cloud computing. The proposed strong user authentication based on local certification authority is presented in Section 6.

II. USER AUTHENTICATION IN CLOUD COMPUTING SERVICES

Today, most organizations adopt cloud services, they migrate all or part of their infrastructure to the cloud. Moving the infrastructure to the cloud doesn't bring only advantages, it brings its own problems that weren't present in the traditional private infrastructures. Although cloud services have existed in the few past years and a wide majority of companies were using it in daily lives, security is today a serious concern for all companies using cloud services. Authentication is required for in order to restrict illegal access unauthorized users [3].

This security concern discourages some enterprises from migrating their whole infrastructure to the cloud. Nevertheless, the benefits are pervasive enough to migrate at least part of the infrastructure to the cloud. We can solve this security problem by creating and establishing VPN tunnels. Indeed, secured VPN tunnel can be established from the private network (client) to the cloud (server) as it is shown in Figure 1 [8].

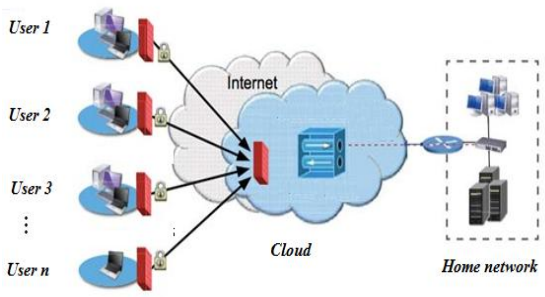

Figure 1. Remote access to cloud services

Authentication is a process through which we can prove and verify the origin of information, the identity of the sender, the identity of a computer or user. Without an efficient authentication rule, we can't manage user access to services, any endpoints can connect to each other without any restrictions. Therefore, it's very important to restrict access allowing the private network to connect to all of the services of cloud servers, and deny access to unauthorized users. In this article, we discuss several techniques used for cloud services authentication, and we propose an efficient and optimal approach.

III. WEAKNESS OF KNOWLEDGE BASED AUTHENTICATION (KBA)

Knowledge based authentication (KBA) typically is simple login and password authentication, it is widely used by web services. As the name suggests, this technique requires the knowledge of private information of the individual to prove that the person providing the identity information is the owner of the identity. An organization using KBA must collect the secret to be shared between the provider and customer. This secret is stored in the provider's server, and it will be changed only when the customer comes back to access the account. This method ensures authentication by comparing the secret given by the customer to the secret stored in the server.

It is technically easy to discover the user's password. Indeed, using tools available on the internet it is quite easy to discover session passwords, brute force attack is the famous attack of knowledge based authentication. This attach is also known as exhaustive search, so password brute forcing works by an attacker who tries to explore all possible passwords of the user [10]. More password is simple, more it will be easy and quick to find out, For complicated passwords, the attacker should try millions of passwords by testing every combination of letters, digits, special symbols and punctuation symbol until a password is found. So, an attacker will require years, and in some cases hundreds or thousands of years, to completely reveal complicated passwords [9, 10]. There are other sophisticated attacks used to steal user passwords quickly and easily even if the password is long and complicated. Sniffing attacks and man in the middle attacks are widely used by hackers [11]. One time password (OTP) has been used to replace KBA technique, which is typically weak.

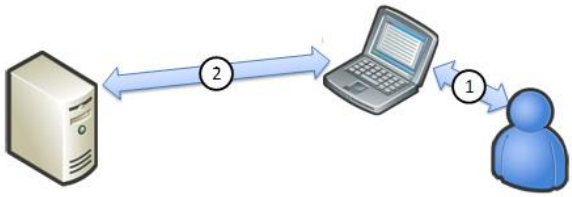

Figure 2. Knowledge based authentication

IV. WEAKNESS OF CONVENTIONAL ONE TIME PASSWORDS (OTP)

With Knowledge based authentication (KBA), it is possible for an attacker to replay the same password once it is intercepted. To avoid this vulnerability, we use one time password (OTP) to limit the validity of the password. Indeed, for each session or transaction, the user sends a different password generated by an OTP calculator (algorithm). This mechanism requires access to something a person has as well as something that a person knows (such as a PIN).

The same algorithm runs independently on the server side and on the client side. This algorithm provides a new password for single use in the client side, the same password is given by the algorithm in the server side [12].

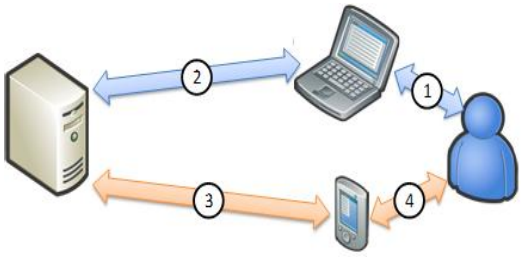

Figure 3. One time password (OTP)

OTP is a password that is valid for only one login session or one transaction. The most important advantage of OTP is that, they are not vulnerable to replay attacks. This means that a hacker who manages to discover an OTP that was already used to log into a service will not be able to use it, since it will be replaced by another. A second major advantage is that a user who uses the same password for multiple systems, is not made vulnerable on all of them, if the password for one of these is discovered by an attacker. OTP approach aim to ensure that a session password cannot easily be intercepted without knowledge of unpredictable information created during the previous session [13].

OTP technique uses software calculators that are vulnerable, if the user's secret is known, a hacker can download the calculator used by OTP, and then that hacker may generate OTP used for authentication. Moreover, it is possible to steal OTP using password brute forcing.

V. WEAKNESS OF CONVENTIONAL STRONG USER AUTHENTICATION IN CLOUD COMPUTING

Strong user authentication refers to combination of two or more classes of human authentication factors:

- Something known to only the user (knowledge based): password, shared secrets, PIN…;
- Something held by only the user (possession based): security token, smart card, mobile device...;
- Something inherent to only the user (biological or behavior biometric): facial recognition, fingerprint, voice recognition…

The combination of the two known and held factors makes up the strong authentication method, and significantly improves the authentication strength, as it secure against the threat of stolen digital identities.

Today, an organization's security policies will include capabilities to live in the cloud computing. Although cloud services do not reside in an organization's own infrastructure, the same integration concerns security access control. However, implementing conventional strong user authentication involves the deployment of hardware tokens, such as smart cards. This technique is useful for closed communities with limited number of employees and partners. Moreover, these strong user authentication methods are difficult to manage and too costly for cloud computing environment. That's why strong user authentication based on certification authority is today more suitable for cloud computing services because this technique doesn't need any hardware deployment [14].

VI. STRONG USER AUTHENTICATION BASED ON LOCAL CERTIFICATION AUTHORITY

Authentication based on digital certificates ensures authentication using a public and private encryption key. Public key is made available to everyone via a publicly accessible directory or database, but private key is secrete and unique to the device or the person who possesses it. In asymmetric encryption, a certification authority (CA) is an entity that delivers digital certificates. A digital certificate certifies the ownership of a public key by the user subject of the certificate.

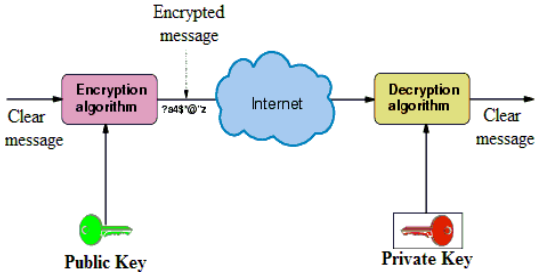

Figure 4. Public key encryption diagram

This method can also be used to digitally sign transactions and to ensure non repudiation. Digital certificates can be delivered by USB tokens, smart cards or simply by mail. In this section, we will present strong user authentication based digital

signature, and then we will present proposed authentication based on local certification authority [15].

A. *Strong user authentication based digital signature*

The digital signature is the equivalent of a hand written signature, but it offers more security. Digital signatures are used to verify transactions origin or senders, it is a mathematical scheme to verify the authenticity of digital messages or documents.

Digital signatures are based on public key encryption, to create a digital signature for a message, we first create a hash of this message which will be signed (using hashing algorithm such as MD-5, SHA-1 or SHA-2), and then the private key is used to encrypt the hash. The encrypted hash is the digital signature. The receiver decrypts the encrypted hash using sender's public key, so the receiver can be sure of the sender's identity and that the data arrived intact [16].

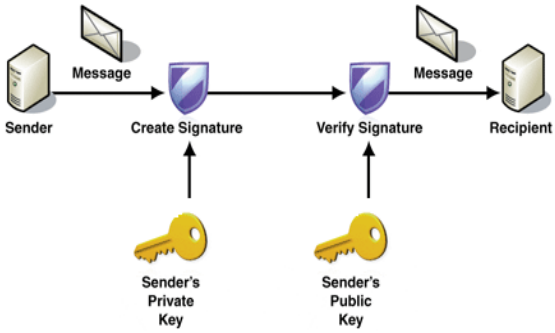

Figure 5. Digital signature process

The reason for encrypting the hash instead of the message is that a hashing algorithm can convert an arbitrary input into a fixed short length value. Today in many countries, including Morocco, digital signatures have the same legal significance as the traditional forms of signed documents.

B. *Proposed strong user authentication based on local certification authority*

The certification authority (CA) is a trusted party organization or company that delivers digital certificates used to create digital signatures and public/private key pairs. The CA guarantees that a user has the unique public key PAlice, in fact, who he or she claims to have. The CA is a critical component in information security because it guarantee that the two parties exchanging data are really who they claim to be. A digital certificate is used to verify that user identity over public key infrastructure (PKI), it is also referred as public key certificate. The CA delivers an encrypted digital certificate containing the public key and other identification information (name, address …) [16].

Knowing that for most enterprises with worldwide branches, even if the whole infrastructure is in the cloud, the security of data over internet is guaranteed with VPN tunnels (IP Sec, SSL, …), authentication is considered for an internal use between enterprise's users, the certification authority is needed only for internal use. Therefore, we can create a local certification authority and avoid purchasing a commercial certificate.

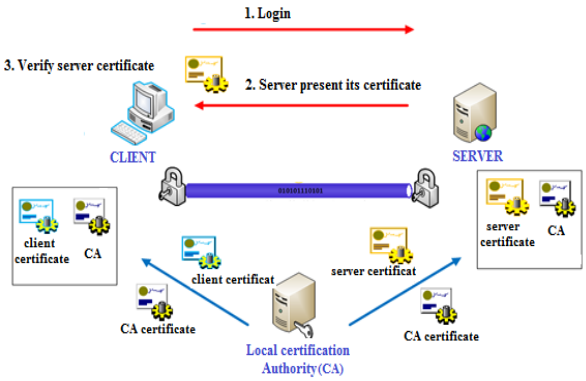

Figure 6. Strong user authentication based on local certification authority

Strong user authentication based on local certification authority is proposed to be used for cloud computing services, because of its level of security, its low cost and its simple structure for cloud services. A mutual authentication client/server is used, client verify the certificate presented by the server while server verify the certificate presented by the client. In this case certification authority is local because there are a limited number of users and all users are known to the company. This approach is adopted because it doesn't require any subscription or purchasing of public certificates for an enterprise with worldwide branches using cloud computing services.

VII. CONCLUSION

The proposed strong user authentication based on local certification authority is specifically tailored to organizations using cloud computing services. The conventional authentication techniques such as knowledge based authentication (KBA) and one time passwords (OTP) are today insufficient to ensure strong security for important cloud services. These conventional methods are vulnerable to sophisticated attacks on the internet (brute force attacks, sniffing attacks, man in the middle attacks…). Moreover, techniques implementing conventional strong user authentication using hardware tokens, are useful for closed communities with limited number of users. These methods are difficult to manage and too costly for cloud computing services. Our method improves the authentication strength without any hardware tokens and it doesn't require any subscription or purchasing of commercial certificates.

VIII. REFERENCES

[1] Hand, Eric, "Head in the Clouds", Nature, Volume 449, Issue 7165, pp. 963, 2007.

[2] Weiss, Aaron. "Computing in the clouds", Magazine netWorker Volume11, issue 4, 16-25, 2007.

[3] Y. Yang, H. Lu, and J. Weng, "Multi-User Private Keyword Search for Cloud Computing", In the Third International Conference on Cloud Computing Technology and Science, pp.264-271, 2011.

[4] Juha Risikko, Nordea. "Strong End-user Authentication for Online Banking with NFC Handsets", IBM, 2009.

[5] Rui Jiang, "Advanced secure user authentication framework for cloud computing", the international journal of smart sensing and intelligent system, volume 6, issue 4, 2013.

[6] R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key. Communications of the ACM, Vol. 21 (2), pp.120–126. 1978.

[7] Wojciech Kinastowski, "Digital Signature as a Cloud-based Service", cloud computing 2013 : The Fourth International Conference on Cloud Computing, grids, and Virtualization, 2013.

[8] Cisco Systems et al. Internet working Technologies Handbook, Third Edition. Cisco Press, p. 232, 2000.

[9] Diffie, Hellman "Exhaustive Cryptanalysis of the NBS Data Encryption Standard", Computer 10, p74–84, 1977.

[10] Robert Reynard, "Secret Code Breaker II: A Cryptanalyst's Handbook", Smith & Daniel Marketing Jacksonville, , 2008.

[11] Tanmay Patange, "How to defend yourself against MITM or Man-in-the-middle attack", 2013.

[12] Jonathan Katz, "Efficient Cryptographic Protocols Preventing Man-in-the-Middle" Attacks", thesis School of Arts and Sciences, Columbia university, 2002.

[13] M. Viju Prakash, P. Alwin Infant and S. Jeya Shobana, "Eliminating vulnerable attacks using one time password and passtext analytical study of blended schema", Universal Journal of Computer Science and Engineering Technology, 1 (2), 133-140, Nov. 2010.

[14] Smart Card Alliance, "Strong Authentication Using Smart Card Technology for Logical Access",A Smart Card Alliance Access Control Council White Paper, 2012.

[15] Bo Yang, "Efficient Certificateless Strong Designated Verifier Signature Scheme", IEEE conference on computational Intelligence and Security,p 432-436, 2009.

[16] Chen Tianhuang,"Digital signature in the application of e-commerce security" IEEE conference on E-Health Networking, Digital Ecosystems and Technologies (EDT), p366-369, 2010.

AUTHORS' INFORMATION

My Abdelkader Youssefi was born in Tinghir, Morocco in 1979. He received the engineering degree in telecommunications from the Posts and Telecommunications National Institute (INPT), Morocco, in 2003, and he received his PhD in computer sciences from EMI School of Engineering, Rabat, Morocco (2015). During 2008-2015, he worked as a computer science engineer. His research interests include Wired/Wireless Networks, cloud computing security and information technology.

